Technique to improve Efficiency of Energy For Data Aggregation using Internet of Things

Synopsis submitted to the IIMT University in partial fulfillment of the requirements for the award of the Degree of

DOCTOR OF PHILOSOPHY

In

(CSE)

By

(MANISHA PUNDIR SAJWAN)

Full time

Under the guidance of

Dr. Suraj Mallik

&

Dr. Seema Nayak

School Of Engineering and Technology

IIMT University, Meerut

IIMT University, Meerut

(Department of Computer Science and Engineering, School of Engineering and technology)

(Feb 2023)

List of Pages

- Introduction
- Literature review
- Objective of work including Scope of Study and hypotheses
- Methodology or your work plan
- Conclusion
- Bibliography or references

ABSTRACT

The IoT having function dispersed from a central to local authorities where sometimes nodes join or leave according to requirement of the network. The energy consumed by these sensor nodes is the big problem of IOT networks because the size of small nodes and far deployment. This complete network structure is divided into some clusters and each cluster is of same size. according to sensor nodes and distance Head of clusters is selected in each cluster. For data aggregation a hierarchical technique is being used which uses least network energy. The sensor nodes positions will be localized by the base station and next hop is selected by sensor nodes for transmission of data. We found that this gateway nodes will be deployed in between each level. The proposed technique decreases routing overhead which decreases consumption of power of network. Thisbreakthrough technique will be implemented in MATLAB.

Chapter 1

Introduction

1.1 Introduction to IOT Network

1. The fundamental idea behind IoT is to enhance the capabilities of devices and objects by enabling them to gather and share data in real-time, thus creating a more interconnected and intelligent world. By leveraging sensors, actuators, and network connectivity, IoT devices can monitor their surroundings, make informed decisions, and take automated actions based on the data they collect.
2. The potential applications of IoT are vast and span across various domains such as healthcare, agriculture, transportation, manufacturing, smart homes, and cities. In agriculture, IoT can assist farmers in monitoring soil moisture levels, optimizing irrigation, and improving crop yields. In smart homes, IoT devices can control appliances, lighting, and security systems, offering convenience and energy efficiency.
3. The key components of an IoT system include the physical devices or objects, sensors for data collection, connectivity infrastructure (such as Wi-Fi, Bluetooth, or cellular networks), cloud platforms for data storage and processing, and applications for analyzing and visualizing the collected data. Additionally, IoT security is a critical consideration, as the interconnected nature of devices can present vulnerabilities and privacy concerns.
4. Overall, IoT has the potential to revolutionize industries, improve efficiency, and enhance the quality of life for individuals. As technology continues to advance, we can expect to see an increasing number of IoT devices and applications that shape the way we interact with the world around us.

1. Calculate the important environmental conditions such as temperature, pressure and humidity as well as other physical conditions.
2. Operate various devices that help in controlling the conditions.
3. Provide communications that are efficient and reliable.

Sensor nodes are having two kinds. One is the sensor node and another is sink node. First the data is sensed and then collected by different nodes. After that collected data is passes to the sink node.

In the wireless sensor node architecture has a sensing, a processing, a power and communication unit. The data is sensed by sensing unit, processed by processing unit and communicated by communicated unit. The sensing unit also sense environment. Then, the resultant information is transmitted between nodes through communication unit. There is a battery for energy resource. These batteries have less amount of power and there is no possible way to exchange battery. So, power consumption plays a vital role in IOT network.

1.1.2 Characteristics:

1. Data Collection and Analysis: IoT devices gather vast amounts of data from the physical world. This data is collected, processed, and analyzed either locally on the device or in the cloud, providing valuable insights and enabling intelligent decision-making.
2. Automation and Control: IoT devices can be remotely monitored, controlled, and managed. They can be programmed to perform automated tasks based on predefined conditions or user preferences, enhancing efficiency and convenience.
3. Scalability: IoT networks can accommodate a large number of devices, ranging from a few to millions, providing scalability for various applications and environments.
4. Real-time Capabilities: IoT systems often require real-time or near real-time responses to changing conditions. This enables immediate actions and enhances responsiveness in critical scenarios.
5. Security and Privacy: With the vast amount of data being collected and transmitted, security and privacy are crucial considerations in IoT. Measures such as encryption, authentication, and access controls are implemented to protect the integrity and confidentiality of data.
6. Ubiquitous Connectivity: IoT devices can be connected and accessed from anywhere, anytime, using various communication technologies like Wi-Fi, cellular networks, Bluetooth, or Low-Power Wide Area Networks (LPWANs).

These characteristics of IoT contribute to its widespread adoption and the creation of a more interconnected and intelligent world.

1.1.2 Design issues

The design of IoT systems involves several key considerations and challenges. Here are some design issues that need to be addressed when developing IoT solutions:

1. Interoperability: IoT devices and platforms often come from different manufacturers and use various communication protocols. Ensuring interoperability and seamless integration between different devices and systems can be a complex task.

2. calability: IoT systems need to handle a large number of devices and data streams. Designing scalable architectures that can accommodate the growth of connected devices and the volume of data is crucial.

3. Security: IoT devices are prone to security threats due to their connectivity and the potential value of the data they collect. Designing hard to break security measure, is essential to protect IoT systems from unauthorized access, data breaches, and malicious attacks.

4. Privacy: IoT Ensuring proper data privacy protection, including data anonymization, user consent mechanisms, and secure data storage and transmission, is crucial to maintain user trust.

5. Data Management and Analytics: IoT systems generate massive amounts of data. Effective data management, including data collection, storage, processing, and analysis, is vital for extracting valuable insights and making informed decisions.

6. User Experience: IoT solutions should be designed with the end user in mind. User interfaces should be intuitive and easy to use, providing a seamless experience for controlling devices, monitoring data, and interacting with the system.

7. Reliability and Fault Tolerance: IoT systems often operate in diverse and dynamic environments. Designing for reliability, fault tolerance, and resilience is important to ensure that the system can handle failures, connectivity issues, and adverse conditions without significant disruption.

8. Standards and Regulations: The IoT landscape lacks universal standards and regulations. Designing solutions that adhere to relevant industry standards, comply with privacy regulations, and ensure data interoperability can help mitigate compatibility issues and legal challenges.

1.2 Energy Consumption in IOT

The sources that cause major wastage of energy in sensor networks are:

Energy consumption is a significant consideration in the design and operation of IoT systems. Here are some factors that influence the energy consumption of IoT:

1. Device Efficiency: The energy efficiency of IoT devices themselves plays a crucial role. This includes the hardware components, such as processors, sensors, and communication modules, as well as the software running on the devices. Optimizing the design and power management techniques at the device level can help reduce energy consumption.

2. Communication Protocols: The choice of communication protocols used in IoT systems can impact energy consumption. Some protocols, such as Wi-Fi and cellular networks, require more power compared to low-power alternatives. Selecting the appropriate protocol for the specific requirements of the application can help minimize energy usage.

3. Data Transmission: The frequency and volume of data transmission between IoT devices and the network or cloud can significantly affect energy consumption. Transmitting large amounts of data frequently can consume more energy. Employing techniques like data compression, data aggregation, and optimizing data transfer protocols can help reduce energy usage during communication.

4. Sleep Modes and Wake-up Mechanisms: IoT devices can be designed to enter low-power sleep modes when not actively performing tasks. By minimizing power consumption during idle periods and using efficient wake-up mechanisms, devices can conserve energy without compromising functionality.

5. Power Sources: The choice of power sources for IoT devices is essential. Some devices rely on batteries, while others may use energy harvesting techniques or direct power sources. Selecting the appropriate power source and considering factors like battery life, rechargeability, and environmental impact can impact the long-term energy consumption of IoT systems.

Chapter 2
Literature Review

Daemin Shin, et.al (2016) shared his reviews in this research paper [12] that Many different services like Smart Home using Internet of Things in which communication device is mobile phones., the PMIPv6 security protocols, does not provide any security for routing whenever external IOT devices are connected with the mobile phones. To ensure security the route for mobile and IOT devices, a new protocol is proposed.

Shuai Zhang, et.al (2017) shared his review in this research paper [13] that in the Internet of Things (IoT), Two factors are considered that is delay and security.With reference of this paper a framework related to delay and security is proposed. The IOT device's location and packets arrival are framed using adopting stochastic geometry and queuing mechanisms.

Chapter 3

Problem Formulation

The IOTnetworks are the localized network in which these sensor nodes recognize the information and forward it to base station. The consumption of power is the important issues of the sensor network due to far deployment and small size of the sensor nodes. The hierarchal routing protocol is the power capable that does not have any structure data aggregation protocol. The hierarchal routing protocol has three phases, in the first phase the hello message is being sent by base station to each node. Thennode reply back to base station with their address and other information. In the second phase, complete network is separated into hierarchal structure network density. In the third phase, the hop is getting selected on the basis of the next node buffer size, residual energy and link strength.

3.1. Objectives

Following are the research objectives: -

1. Implementation ofhierarchal routing protocolpower throughput routing protocol to increase lifetime and decrease routing overhead in IOT networks

2. To increasehierarchal routing protocolpower throughput routing protocol to increase lifetime and decrease routing overhead in wireless sensor networks

3. Implementation of proposed protocol and comparison with existing parameters.

3.3. Research Methodology

The IOT networks is the self-configured network in which sensor nodes gets information and forward it to base station. The hierarchal routing protocol is the protocol which works in the three phases for the data aggregation. the base station will send the hello message to each node in the network to gather its information. In the second phase, the base station will define the level of each node on the basis of their density. In the third phase on the basis of their residual energy, buffer size and link stability factor node is being chosen. In the research work, between each level, the leader nodes are selected on the basis of distance. The leader's nodes are the data forwarding nodes which forward the data of one level to next level. The proposed improvement leads to reduction in routing overhead and energy consumption of the network.

Chapter 4

Facilities Required

Following are the various facilities required for this project :-

1. Hardware Requirements

- Dual Core Processor
- 4 GB RAM
- 128 GB Hard Disk

2. Software Requirements

- MATLAB (2015 version or above)
- Microsoft Word
- Windows

Conclusion

To improve energy efficiency in data aggregation for IoT, several techniques can be implemented. These techniques aim to minimize the energy consumption associated with data transmission and processing while ensuring the accuracy and reliability of aggregated data. In conclusion, here are some key points to enhance energy-efficient data aggregation in IoT:

1. Data Filtering and Sampling: Filtering and sampling techniques can be applied to IoT data to remove redundant or less critical information before transmission. By selectively transmitting relevant data or aggregated summaries, energy consumption can be reduced.

REFERENCES

[1]I.F.Akyildiz,W.Su,Y.Sankarasubramaniam,E.Cayirci. "WirelessSensorNetworks:Asurvey" Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgiainstituteof Technology,Atlanta,GA 30332,USAReceived12December2001; accepted20 December2001, pp . 392-422.

[2] G.H. Raghunandan, B.N. Lakshmi, "A Comparative Analysis of Routing Techniques for Wireless Sensor Networks", Proceedings of the National Conference on Innovations in Emerging Technology,IEEE 2011.

[3] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009, pp. 1-9

[4] Sneha Kamble and Tanuja Dhope, "Reliable Routing Data Aggregation using Efficient Clustering in WSN ", International Conference on Communication Control and Computing Technologies,IEEE,2017,pp.246-250

[5] Alka Singh, Shubhangi Rathkanthiwar and Sandeep Kakde, "Energy Efficient Routing of WSN using ParticleSwarm Optimization and V-Leach Protocol", International Conference on Communication and Signal Processing,IEEE,2016,India

[6] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks" Journal of Security Engineering, 2014, pp.241-250

[7] Roshan Singh Sachan, Mohammad Wazid, Avita Katal, D P Singh, R H Goudar, "A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN", International conference on Communication and Signal Processing, April 3-5, 2013, India

[8] Yi-Ying ZHANG, Xiang-zhen LI, Yuan-an LIU, "The detection and defense of DoS attack for wireless sensor network", Elsevier Journal of China Universities of Posts and Telecommunications, Vol19, pp. 52-56, Oct-2012.

[9] Kalpana Sharma and M K Ghose, “Wireless Sensor Networks: An Overview on its Security Threats”IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010, pp.42-45

[10] Guoxing Zhan, Weisong Shil, Julia Deng, “TARF: A Trust-Aware Routing Framework for Wireless Sensor Networks”, EWSN 2010, LNCS 5970, pp. 65–80, 2010.

[11] Hailun Tan, Diethelm Ostry, JohnZic, SanjayJha, “A Confidential and DoS-Resistant Multi-hop Code Dissemination Protocol for Wireless Sensor Network”, ACM WiSec09, Zurich, Switzerland, March 16-18, 2009

[12] Daemin Shin, Vishal Sharma, Jiyoon Kim, Soonhyun Kwon, and Ilsun You, “Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Networks”, 2016, IEEE

[13] Shuai Zhang, Jianhua Peng, Kaizhi Huang, Xiaoming Xu and Zhou Zhong, “Physical Layer Security in IoT: A Spatial-TemporalPerspective”, 2017, IEEE

[14] Dr. Reshma Banu, Dr. G. F. Ali Ahammed, Nasreen Fathima, “A Review on Biologically Inspired Approaches toSecurity for Internet of Things (IoT)”, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016

[15] Minela Grabovica, Dražen Pezer, Srdan Popic, Vladimir Kneževic, “Provided security measures of enabling technologiesin Internet of Things (IoT): A survey”, 2016, IEEE

[16] Zimu Guo, Nima Karimian, Mark M. Tehranipoor and Domenic Forte, “Hardware Security Meets Biometricsfor the Age of IoT”, 2016, IEEE

[17] José L. Hernández-Ramos, Jorge Bernal Bernabe, Antonio F. Skarmeta, “Managing Context Information for Adaptive Securityin IoT environments”, 2015 29th International Conference on Advanced Information Networking and Applications Workshops